# 关于共享机器的入侵过程

2001-03-08.02:32:32

http://www.cnhonker.com

Honker Union of China

大家好！

上次给大家的教程有一种方法要用到net use。

现在给大家我亲自写的第二篇教程，来介绍一下关于共享机器的入侵过程。

首先，我们要准备一个工具。

legion 2.1

大家可以到这里下载。http://warex.box.sk/files/scanners/legion.zip

因为本站的软件下载空间没有落实好，现在还不能放软件。不过就会建设好了。

大家在国内的很多所谓黑客网站也可以找到。

你也可以用

网络刺客二:http://rina.yofor.com/cgi-bin/download/software.cgi?job=click&userno;=1000802023837&id;=3

Smbscanner:http://warex.box.sk/files/scanners/smbscanner.zip

我觉得还是legion 2.1好用一些。

下面就用legion 2.1来介绍一下入侵过程。

注意： 为了你的安全，下载完后请杀毒。

废话少说，让我们来试试通过共享来进入别人机器吧。

噢，别急。

让我们来学一些基础知识吧。

：P

大家需要关于net令的知识。

在这里我只简单说一下。

详细情况大家可以到我的主页的资料文摘的命令指南里找。

http://202.103.69.85/city/asp/word/bug.asp?owner=A106

先说一些：

(1)NET命令是一个命令行命令。

(2)管理网络环境、服务、用户、登陆等本地信息

(3)WIN 98，WIN WORKSTATION和WIN NT都内置了NET命令。

(4)但WIN 98的NET命令和WORKSTATION、NT的NET命令不同。

(5)WORKSTATION和SERVER中的NET命令基本相同。

(6)获得HELP

(1)在NT下可以用图形的方式，开始-》帮助-》索引-》输入NET

(2)在COMMAND下可以用字符方式，NET /?或NET或NET HELP得到一些方法

相应的方法的帮助NET COMMAND /HELP或NET HELP COMMAND 或NET COMMAND /?

另对于错误NET HELPMSG MESSAGE#是4位数

(7)强制参数 所有net命令接受选项/yes和/no(可缩写为/y和/n)。[简单的说就是预先给系统的 提问一个答案]

(8)有一些命令是马上产生作用并永久保存的，使用的时候要慎重

(9)对于NET命令的功能都可以找到相应的图形工具的解决方案

(10)命令的组成 命令 参数 选项  参数 选项  参数 选项 ...

罗嗦说了一大堆，其实就是6和7有用，呵呵

另有两件事：

(1)在NT的NET命令中有一些参数是只有在SERVER环境中才能使用的

(2)在WIN98的NET命令中有一些参数不能在DOS-WIN中使用，只能在DOS环境中使用

下面对NET命令的不同参数的基本用法做一些初步的介绍：

(1)NET VIEW

作 用：显示域列表、计算机列表或指定计算机的共享资源列表。

命令格式：net view [\\computername  /domain[:domainname]]

参数介绍：

(1)键入不带参数的net view显示当前域的计算机列表。

(2)\\computername 指定要查看其共享资源的计算机。

(3)/domain[:domainname]指定要查看其可用计算机的域。

简单事例：

(1)net view \\host查看host的共享资源列表。 host可以为IP,也可以为域名。

(2)net view /domain:LOVE查看LOVE域中的机器列表。

(3)NET USE

作 用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：net use [devicename  *] [\\computername\sharename[\volume]] [password  *]] [/user:[domainname\]username] [[/delete]  [/persistent:{yes  no}]]

参数介绍：

键入不带参数的net use列出网络连接。

devicename指定要连接到的资源名称或要断开的设备名称。

\\computername\sharename服务器及共享资源的名称。

password访问共享资源的密码。

*提示键入密码。

/user指定进行连接的另外一个用户。

domainname指定另一个域。

username指定登录的用户名。

/home将用户连接到其宿主目录。

/delete取消指定网络连接。

/persistent控制永久网络连接的使用。

简单事例:

(1)net use e: \\host\TEMP将\\host\TEMP目录建立为E盘

(2)net use e: \\host\TEMP /delete断开连接

(3)net use \\host "password" /user:"administrator"

至于其它的net time, net print ,net file 等等命令在这里都用不到。就不说了。

共享主机

所谓的共享主机就是在计算机里有共享的硬盘，文件夹或是打印机等共享项目。

只在安装了网卡的计算机上才可以设置共享，如网吧 公司里的局域网和一些人自己连的对等网。个人可以在我的电脑里在硬盘上点激鼠标右键来看看是否有共享这一项，如果有则可以在里面对自己的共享进行设置。

共享的设置可以分为只读（可以对硬盘文件进行读取但无法删除或是上载） 完全（可以读取 删除 上载等操作）需要密码访问（对上面的两种操作分别来设置密码）。

不可否认共享在局域网上是给我们带来了很大方便但如果开着共享的主机直接连上互联网的话就会给安全带来很大的隐患了。

首先如果你是台WIN98的话想要进入互联网上其他的共享主机的话，就要看看你的桌面上有没有网上邻居这一项，在个人安装98的时候默认是没有安装的，如果没有的话就在控制面板里添加删除程序里把通讯一项全部选中然后用98的光盘来进行安装工作。

等一切做好了以后我们就可以开始上网寻找网上的共享主机了，当然首先如果你想要先在自己的局域网内找找共享的话就可以省很多时间了。

当然反过来如果你并不想让对方看到你开着工享的话，可以在本地主机上将共享名称的后面加上一个简单的$号来实现隐藏自己的共享，比如之前你将C 盘共享取了一个名字为C，则现在可以将名称改为C$以后，就不会在网上邻居中再显示你这个共享目录了。但对方依然可以在开始菜单的运行里通过打入\ \你的IP\C$ 来访问你的共享文件，所以可见取个不易被猜到名称也的确是非常重要的。

在网上开着共享的主机多是一些网吧和公司局域中的电脑用户，他们在平时工作中设置共享多是为了玩游戏或是工作需要等，但实际上如果你的共享资源没有加上口令的话。那么全世界的人都可以共享了。可是否有访问密码就安全了呢？抱歉答案依然是否定的，这是由于WINDOWS95，98共享目录密码校验有BUG，可以让其只校验密码第一个字节。如果你是WIN98系统，拷贝一个经过改动的驱动文件到WINDOWS\ SYSTEM目录覆盖原文件，重起机器。（很多地方有这个驱动程序的，不过我暂不提供。）。然后你进入有密码的共享目录出来提示输入密码窗口时不用敲密码，只要按住回车键不放，直到进入此目录。注意出来密码不对提示，你按住回车键不放，就选了确定，再下一回密码，你最多试密码2 56次。一般密码是字母0X20-0X80，就最多96次了。只要你按住回车键不放很快的。远程开了137，139什么的你可以在网络邻居里面输入\\IP,一样的可以。可是WINNT机器不能进入。

我们开始吧。

：P

net view 命令是在windows 的Ms-dos下输入net view \\host 来运行，但为了简单一点，不做大量重复的无聊的工作，我们用软件来找。

我们用winzip把下下载回来的legion 2.1，解压。

然后我们来运行它。

它有两个菜单项，你可以看到关于这个软件的使用和版权等。

你可以先读一下作者的帮助。

然后，在主界面里，我们可以看到。

写着scan type扫描类型 的框

里面有两个单选项，一个是scan Range扫描范围，就是扫描一段ＩＰ地址。 另一个是scan list扫描列表，是对一个文本文件里的文件里的ＩＰ列表来进行扫描的。默认是选的scan range这里我们不改它。

下面的是一个connection speed连接速度。

里面有slower（慢），28.8Kps，56Kps，faster快。

你可以根据你的网速来调整。

这里我们选到56Kps ，当然你如果是教育网接入，或者你扫描局域网里的机器，我们就可以选faster.最快的，让我们的扫描速度更快。

右边的一个是两个IP编辑框，我们输入要扫描的IP范围。

比如

203.203.1.1------203.203.1.254扫描一个Ｃ类IP

或者是

203.203.1.1------203.203.254.254 扫描一个Ｂ类IP.

但我建议你只扫一个Ｃ类，那样快一些。如果你扫Ｂ类，我不相信你有能力能等到它扫描结束。它要花的时间太多了。

好了，先喝杯咖啡吧，等几分种我们再回来。

- - - - - - - - - - - - - - - - - - -

几分钟后，我们回来。

发现在程序主界面的左边和右边都出现了一些字符

其中左边的是找到有共享的ＩＰ地址。右边的是找到共享数目。

一般在右边的是\\ip\找到的共享名。

很多共享你会发现\\ip\c \\ip\d \\ip\e等的。

那样的共享一般是别人共享了整个Ｃ，Ｄ，Ｅ盘的。

我们来看一个\\ip\c的。

在左边的ＩＰ列表中，我们找到ＩＰ下面有Ｃ盘符的。

然后点击Map drive 映射网络盘。它会弹出一个窗口提示你\\ip\c已经被映射成Ｇ或者其他盘

符了。

现在我们的可以在我的电脑里找到一个网络盘G。

象平时我们打开C盘等一样，我们点击就可以进去。

然后，我们就可以进行操作了。

比如把c:\windows*.pwl拷贝到自己的机器上。

然后用pwltools 破解。现在是3.0版。

你可以在这里找到它。

http://rina.yofor.com/cgi-bin/download/software.cgi?job=click&userno;=1000802020420&id;=3

通常你可以用它找到开机密码，上网密码等。

C :\WINDOWS\Application Data\Identities\{3E690B40-97EA-11D4-967B-9117A21ED870}\Microsoft\Outlook Express是放outlook的新邮件的地方，你可以用写字板来查看它。

如果他们把共享设成完全共享的话。

那么你不止可以拷贝他的文件，你还可以给它的机器放文件！

比如我在他的。c:\windows\Start Menu\programs\启动\里放上冰河的服务器端。

下次开机时他的机器就会自动运行这个文件了。

：P

然后你的冰河就可以为你提供更强大的控制了。

再然后呢，他的上网密码，FTP密码，信箱密码等等都逃不了啦。

现在新的改造过的冰河已经可以逃过很多杀毒软件了。

这一课是给刚入门的新手的，也是最简单的入侵方法，没什么技术可言。：P

以后我将陆续给大家写教程。并通过《中国红客网络安全技术联盟》的邮件列表发给大家。

如果你订了我们的邮件不能收到我们的教程，那么请用另外一个信箱重新订阅。

建议大家用www.21cn.com的信箱。

如果你到现在都没有订我们的邮件列表的话，请你尽快到我们红客联盟的主页订取。
http://www.cnhonker.com

附件里的是我刚才为了写教程才找到的几个共享主机。在教程里就不贴了。大家尽快连接吧。

这也是为什么要订邮件列表的原因。

我的下一篇教程预告是　关于允许匿名登陆的主机攻击
如果你有什么想法和建议请你写信到：bunny_lion@21cn.com。

by Lion

OICQ:5437211
bunny_lion@21cn.com

欢迎访问：
《中国红客网络安全技术联盟》
http://www.cnhonker.com　　主站点
http://coollion.3322.net　　镜像站

2000/11/26

cnhonker.com.

>>相关资料

关闭本窗口